DRAFT INTERNATIONAL STANDARD

ISO/SAE DIS 21434

ISO/TC **22**/SC **32** Secretariat: **JISC**

Voting begins on:
2020-02-12

Voting terminates on:
2020-05-06

Road vehicles — Cybersecurity engineering

ICS: 43.040.15

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/SAE DIS 21434:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

SAE International
400 Commonwealth Dr.
Warrendale, PA, USA 15096
Phone: 877-606-7323 (inside USA and Canada)
Phone: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
Website: www.sae.org

Published in Switzerland by ISO, published in the USA by SAE International

CONTENTS

FOREWORD

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

SAE Technical Standards Board Rules provide that: “This document is published to advance the state of technical and engineering sciences. The use of this document is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user.”

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was jointly prepared by Technical Committee ISO/TC 22, Road vehicles, Subcommittee SC 32, Electrical and electronic components and general system aspects, and SAE Vehicle Cybersecurity Systems Engineering Committee.

This first edition of ISO/SAE 21434 cancels and supersedes SAE J3061_201601.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html. Alternatively, to provide feedback on this document, please visit http://standards.sae.org/PRODCODE.

INTRODUCTION

Purpose of this Document

This document addresses the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with changing technology and attack methods.

This document provides vocabulary, objectives, requirements and guidelines as a foundation for common understanding throughout the supply chain. This enables organizations to:

- define cybersecurity policies and processes;
- manage cybersecurity risk; and
- foster a cybersecurity culture.

This document can be used to implement a cybersecurity management system including cybersecurity risk management in accordance with ISO 31000. This document is intended to supersede SAE J3061 recommended practice.

Organization of this Document

An overview of the document structure is given in Figure 1. The elements of Figure 1 do not prescribe an execution sequence of the individual topics.

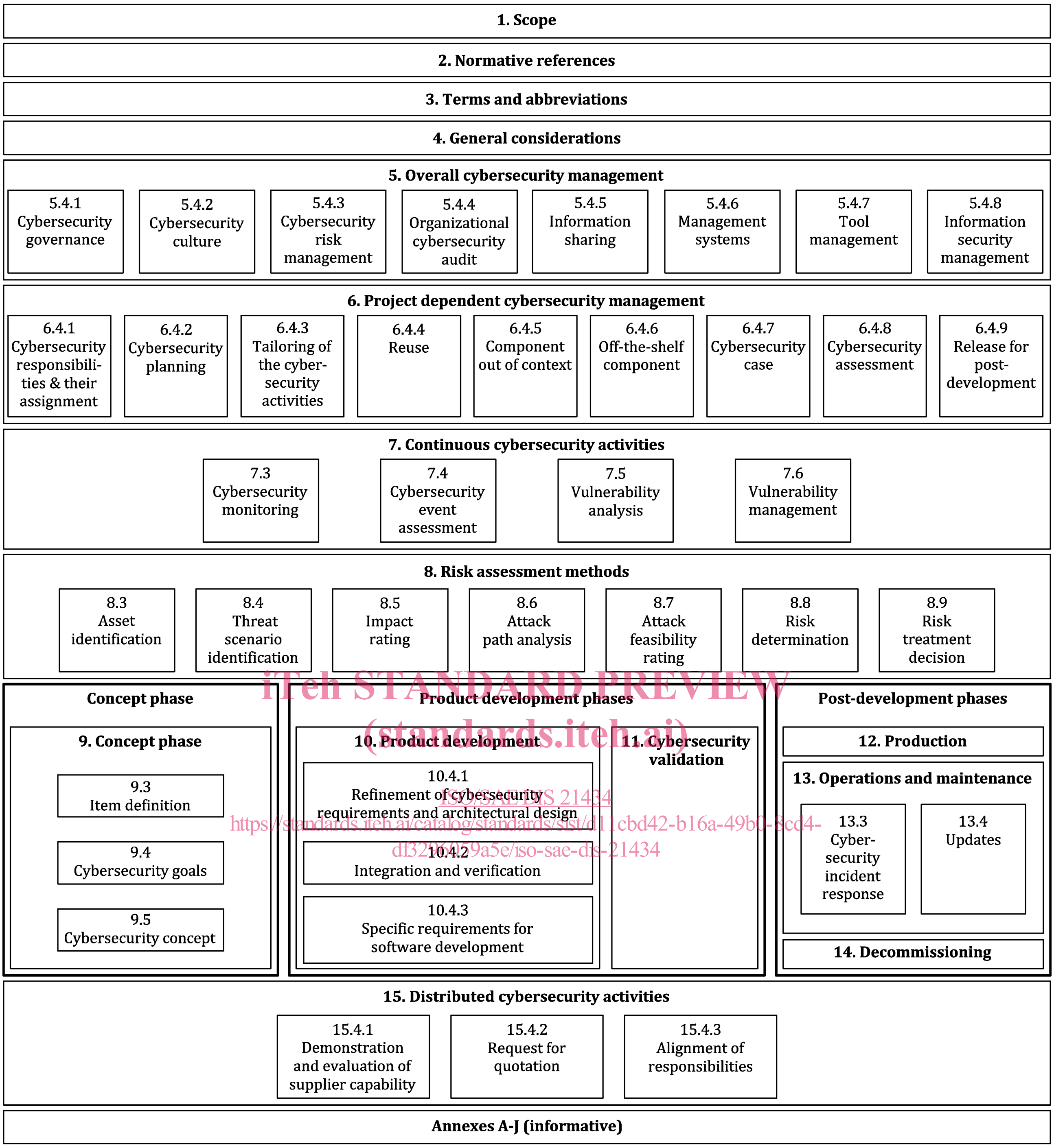
1. Scope
2. Normative references
3. Terms and abbreviations
4. General considerations
5. Overall cybersecurity management
5.4.1 Cybersecurity governance
5.4.2 Cybersecurity culture
5.4.3 Cybersecurity risk management
5.4.4 Organizational cybersecurity audit
5.4.5 Information sharing
5.4.6 Management systems
5.4.7 Tool management
5.4.8 Information security management
6. Project dependent cybersecurity management
6.4.1 Cybersecurity responsibilities & their assignment
6.4.2 Cybersecurity planning
6.4.3 Tailoring of the cybersecurity activities
6.4.4 Reuse
6.4.5 Component out of context
6.4.6 Off-the-shelf component
6.4.7 Cybersecurity case
6.4.8 Cybersecurity assessment
6.4.9 Release for post-development
7. Continuous cybersecurity activities
7.3 Cybersecurity monitoring
7.4 Cybersecurity event assessment
7.5 Vulnerability analysis
7.6 Vulnerability management
8. Risk assessment methods
8.3 Asset identification
8.4 Threat scenario identification
8.5 Impact rating
8.6 Attack path analysis
8.7 Attack feasibility rating
8.8 Risk determination
8.9 Risk treatment decision
Concept phase
9. Concept phase
9.3 Item definition
9.4 Cybersecurity goals
9.5 Cybersecurity concept
Product development phases
10. Product development
10.4.1 Refinement of cybersecurity requirements and architectural design
10.4.2 Integration and verification
10.4.3 Specific requirements for software development
11. Cybersecurity validation
Post-development phases
12. Production
13. Operations and maintenance
13.3 Cyber-security incident response
13.4 Updates
14. Decommissioning
15. Distributed cybersecurity activities
15.4.1 Demonstration and evaluation of supplier capability
15.4.2 Request for quotation
15.4.3 Alignment of responsibilities
Annexes A-J (informative)

Figure 1 - Overview of this document

Clauses 5 and 6 (Management of Cybersecurity) include the implementation of the organizational cybersecurity policy, rules, and processes for overall cybersecurity management and for project dependent cybersecurity management.

Clause 7 (Continuous Cybersecurity Activities) defines activities that provide information for ongoing risk assessments and vulnerability management of E/E systems until end of support.

Clause 8 (Risk Assessment Methods) defines methods to determine the extent of cybersecurity risk.

Clause 9 (Concept Phase) defines an item and the relevant assets, provides cybersecurity risk determination, and defines the cybersecurity goals.

Clause 10 (Product Development) defines the cybersecurity specification, implements and verifies cybersecurity requirements specific to an item or component.

Clause 11 (Cybersecurity Validation) describes the cybersecurity validation of an item at the vehicle level.

Clause 12 (Production) specifies the cybersecurity related aspects of fabrication, assembly and/or calibration of an item or component.

Clause 13 (Operations and Maintenance) specifies activities related to cybersecurity incident response and updates to an item or component.

Clause 14 (Decommissioning) includes cybersecurity considerations that relate to the decommissioning of an item or component.

Clause 15 (Distributed Activities) includes requirements for supplier management.

1. SCOPE

This document specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) systems, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces whose development or modification began after the publication of the document.

This document does not prescribe specific technology or solutions related to cybersecurity.

2. NORMATIVE REFERENCES

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, Risk management - Guidelines

ISO 26262-3:2018, Road vehicles - Functional Safety - Part 3: Concept phase

3. TERMS AND ABBREVIATIONS

3.1 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

ISO Online browsing platform: available at http://www.iso.org/obp

IEC Electropedia: available at http://www.electropedia.org/

3.1.1 ASSET

Something for which the compromise of its *cybersecurity properties* (3.1.17) can lead to damage to an *item's* (3.1.21) *stakeholder* (3.1.29).

3.1.2 ATTACK

Attempted deliberate action or interaction with the item or component or its environment that has the potential to result in an adverse consequence.

3.1.3 ATTACK FEASIBILITY

Qualified attribute of an *attack path* (3.1.4) describing the ease of successfully carrying out the corresponding *attack* (3.1.2).

3.1.4 ATTACK PATH

Set of actions that could lead to the realization of a *threat scenario* (3.1.31).

3.1.5 ATTACKER

Person, group, or organization that conducts an *attack* (3.1.2).

3.1.6 AUDIT

Examination of an implemented process to determine the extent to which the process objectives are fulfilled.

[Modified from SOURCE: ISO 26262-1:2018[1]]

3.1.7 CUSTOMER

Person or organization that receives a service or product.

[Modified from SOURCE: ISO 9000]

3.1.8 CYBERSECURITY

Road Vehicle Cybersecurity

Condition in which *assets* (3.1.1) are sufficiently protected against threat scenarios to electrical or electronic components of road vehicles and their functions.

Note 1 to Entry: In this document, for the sake of brevity, only the term cybersecurity is used.

3.1.9 CYBERSECURITY ASSESSMENT

Judgement of the achieved degree of *cybersecurity* (3.1.8).

3.1.10 CYBERSECURITY CLAIM

Statement on a *risk* (3.1.25) that is accepted.

Note to Entry: Includes a description of why the risk is acceptable and a specification under which conditions the risk needs to be re-evaluated.

3.1.11 CYBERSECURITY CONCEPT

Collection of allocated cybersecurity requirements which achieve identified *cybersecurity goals* (3.1.14).

3.1.12 CYBERSECURITY CONTROL

Measure that is modifying *risk* (3.1.25).

[Modified from SOURCE: ISO 31000:2018]

3.1.13 CYBERSECURITY EVENT

Cybersecurity information (3.1.15) that has been confirmed as potentially relevant to an *item* (3.1.21) or component.

3.1.14 CYBERSECURITY GOAL

Concept level cybersecurity requirement associated with one or more *threat scenarios* (3.1.31).

Note to Entry: The statement of the cybersecurity goal can refer to an asset, attack path or to the damage scenario associated with the threat scenario.

3.1.15 CYBERSECURITY INFORMATION

Information derived from data collected by the monitoring process for which relevance to an item or component has not been determined.

3.1.16 CYBERSECURITY INTERFACE AGREEMENT

Agreement between *customer* (3.1.7) and supplier concerning distributed cybersecurity activities.

3.1.17 CYBERSECURITY PROPERTY

Attribute of an *asset* (3.1.1) including confidentiality, integrity, and availability.

3.1.18 DAMAGE SCENARIO

Adverse consequence or undesirable result due to the compromise of a *cybersecurity property* (3.1.16) (or properties) of an *asset* (3.1.1), or of a group of *assets.*

3.1.19 EMBEDDED SOFTWARE

Fully-integrated software to be executed on a processing element.

[SOURCE: ISO 26262-1:2018[1]]

3.1.20 IMPACT

Estimate of magnitude of damage or physical harm from a *damage scenario* (3.1.18).

3.1.21 ITEM

System or combination of systems to implement a function at the vehicle level.

[Modified from SOURCE: ISO 26262-1:2018[1]]

3.1.22 OUT OF CONTEXT

Not developed in the context of a specific *item* (3.1.21).

3.1.23 PENETRATION TESTING

Cybersecurity testing in which real-world attacks are mimicked to identify ways to compromise *cybersecurity goals* (3.1.14).

[SOURCE: NIST SP 800-115[21]]

3.1.24 RESIDUAL RISK

Risk (3.1.25) remaining after risk treatment.

[SOURCE: ISO/IEC 27000[9]]

3.1.25 RISK

Effect of uncertainty on *road vehicle cybersecurity* (3.1.8) expressed in terms of *attack feasibility* (3.1.3) and *impact* (3.1.20).

[Modified from SOURCE: ISO 31000:2018]

3.1.26 RISK MANAGEMENT

Coordinated activities to direct and control an organization with regard to *risk* (3.1.25).

[Modified from SOURCE: ISO 31000:2018]

3.1.27 ROAD USER

Person who uses a road, such as a pedestrian, cyclist, motorist, or an actor providing transportation.

3.1.28 SERIES PRODUCTION ROAD VEHICLE

Road vehicle that is intended primarily to be used for public roads and is not a prototype.

Note 1 to Entry: Vehicle type classification can vary between regions.

EXAMPLE 1: A vehicle that is sold for use by the general public.

EXAMPLE 2: A vehicle that is sold to be used amongst the general public.

[Modified from SOURCE: ISO 26262-1:2018[1]]

3.1.29 STAKEHOLDER

Person or organization that can be affected by a *damage scenario* (3.1.18).

[Modified from SOURCE: ISO 31000:2018]

3.1.30 TARGET ENVIRONMENT

Environment on which specific software is intended to be executed.

EXAMPLE 1: For application software the target environment is the microcontroller and its software.

EXAMPLE 2: For embedded software the target environment is the ECU in the system context.

3.1.31 THREAT SCENARIO

Statement of potential negative actions that lead to a *damage scenario* (3.1.18).

3.1.32 TRIAGE

Analysis to determine the relevance of *cybersecurity information* (3.1.15) to an item or component.

3.1.33 TRIGGER

Criterion used by cybersecurity monitoring for *triage* (3.1.32).

3.1.34 VALIDATION

Confirmation, through the provision of objective evidence, that the cybersecurity goals of the item are adequate and are achieved.

[Modified from SOURCE: ISO/IEC/IEEE 15288:2015[14]]

3.1.35 VERIFICATION

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

[SOURCE: ISO/IEC/IEEE 15288:2015[14]]